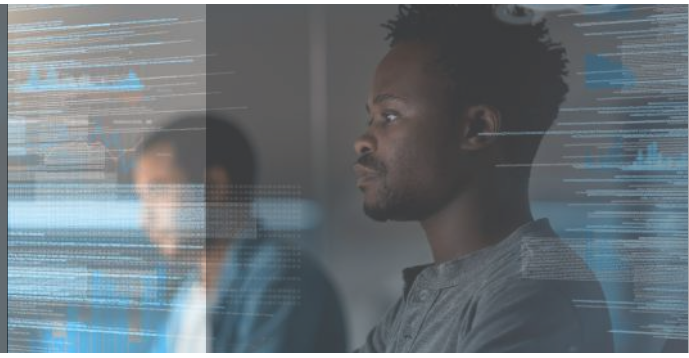
Container Technology Energizes Edge Computing

Modern VxWorks Uses Containers for Intelligent Edge Real-Time Solutions

WNDRVR

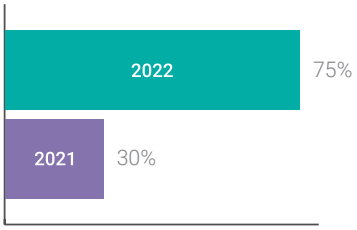
New Opportunities with Container Technology



The security, portability, and agility of container technology complement the proven capabilities of the leading real-time operating system (RTOS), VxWorks®, now available for containerized deployments at the intelligent edge.

As the complexity of applications and their supporting infrastructures create new potential attack vectors for increasingly sophisticated hackers to exploit, containers in embedded systems offer a means to deliver responsive, secure application delivery to the intelligent edge. With these capabilities, aerospace and defense organizations, energy providers, large-scale manufacturers, and medical organizations can take advantage of low-latency, high-bandwidth performance for the most challenging applications.

In an article for ARC Advisory Group titled "Industrial Edge Containers," Harry Forbes noted, "Thinking about these new capabilities and how they might be used, it seems to me that in the longer term, today's sharp border between embedded systems and edge computing will become much blurrier. Indeed, today's real-time embedded applications may eventually become a special case within a broader set of edge applications that are containerized and orchestrated very much the way cloud apps are deployed today."[1]

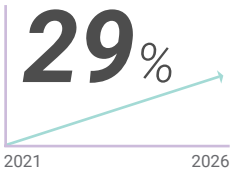


Gartner predicts that by 2022, more than 75% of global organizations will be running containerized applications in production, up from less than 30% today.[2]

1 *Forbes, Harry, "Industrial Edge Containers," ARC Advisory Group, June 2019*

2 *"Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024" (press release), Gartner, June 2020*

One good example of this trend: Avionics systems have evolved from fundamentally hardware-based solutions to agile, highly upgradable, software-defined infrastructures, enabling new technologies to be incorporated into systems on the fly, without substantial hardware replacements. Software container technology promises to be an effective means of countering cybersecurity threats through quick updates and patches, delivering benefits to both the commercial and aerospace/defense sectors. The benefits of software containers, however, can only be fully realized if the security aspects of the technology are well understood and necessary protections are integrated into solutions as part of a DevSecOps process.



Forecast CAGR of the application container market, 2021–2026[3]

> "What about containers at the intelligent edge? Each system runs on a different platform. Maybe VxWorks, maybe Linux, maybe others. How do we make it uniform so there are not workflow changes from system to system? Picture having an edge cloud that lets you push software. This is the vision we are working toward."
>
> — **Michel Chabroux, Senior Director, Product Management, Wind River**

3 *"Global Application Container Market (2021 to 2026)" (press release), ResearchAndMarkets.com, February 2021*

Container Technology Comes of Age

To make it easier to deploy long-lifecycle, embedded solutions that require minimal footprints, Wind River® introduced container technology to Wind River Linux in 2019.

VXWORKS WITH OCI COMPLIANCE

To further strengthen development of mission-critical applications — particularly well suited for edge computing use cases — Wind River recently launched VxWorks with OCI-compliant container support, making it possible to harness the same cloud infrastructure, tooling, and workflow that developers have used in familiar IT environments.

In developing container support for VxWorks, Wind River has pioneered a technological advance for RTOS applications and ushered in a new era, enabling small-footprint embedded solutions that are robust enough for critical edge-computing applications in a variety of industry sectors.

Docker, CoreOS, and other leaders in the container technology field established ground rules for container use and specifications to achieve compliance with open standards. Details on this open standard, as well as tools and sample code, are available through the Open Container Initiative and GitHub repositories.

Open Container Initiative (OCI)

To drive and unify advances in container technology, Docker and others established two specifications: a Runtime specification and an Image specification. The Runtime specification covers unpacking of the downloaded file system bundle, the OCI image. The file system bundle is unpacked into an OCI Runtime file system bundle to be run by the OCI Runtime. VxWorks adheres fully to these OCI specifications.

Learn more.

Autonomous Autos Reshape the Marketplace

Docker, rkt, Railcar, LXC, CRI-O, and other container runtime software rely on a client/host architecture. Figure 1 shows the DevSecOps processes as they apply to VxWorks container implementations.

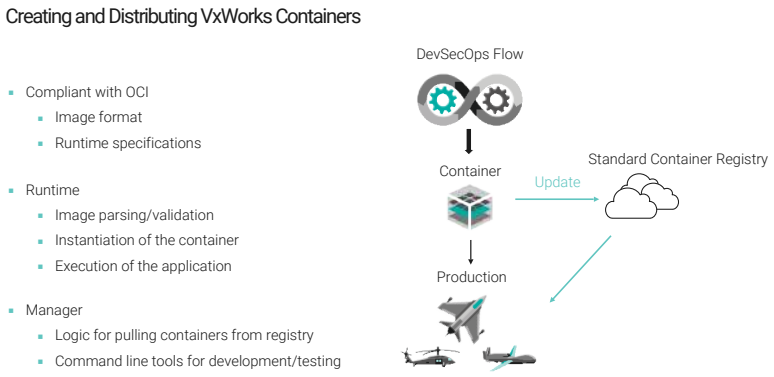


Figure 1. Production process for creating and updating VxWorks-based containers

In a typical DevSecOps environment involving VxWorks-based containers, application code is created using a best-practices security framework. The application is released as a container to a host that is the targeted endpoint, such as a VxWorks-based device, and also to the container registry. Any updates or patches to the code can be pushed to the registry, stored, and then pulled from the registry as needed by the host system, whether an aircraft, a connected car, or an electrical substation — any vehicle, medical device, IoT installation, or manufacturing facility that is using containers for code distribution.

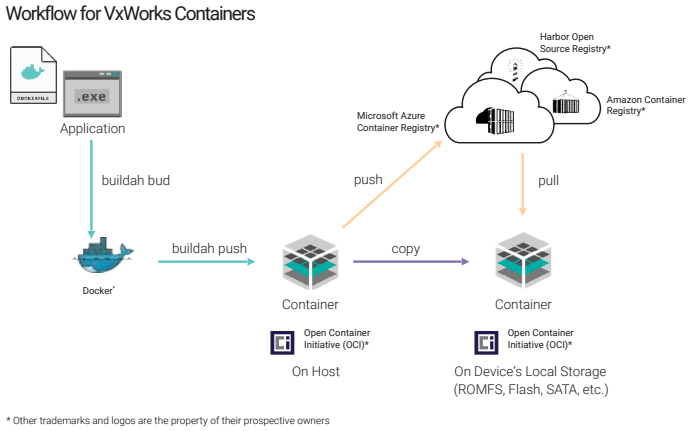
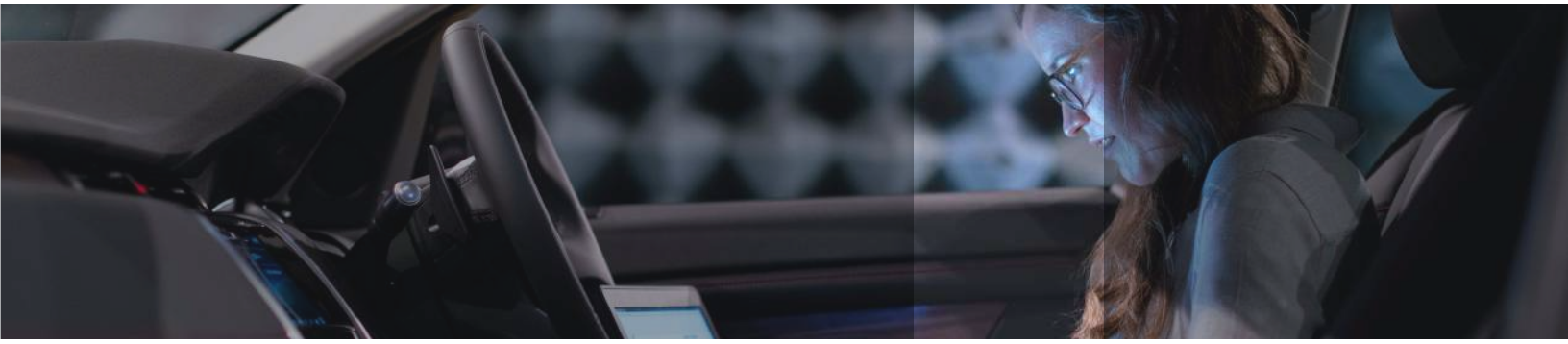


Figure 2. End-to-end workflow creating and distributing containers



Once application binaries have been developed, a standard Docker file is generated. An open-source tool, Buildah, then creates the container image, which is a packaged file bundle containing the components of the application. The container is then pushed to the container registry and copied to the targeted hosts as well. The container registry itself — a Docker hub, Amazon ECR, Harbor, or any other OCI-compliant registry — is available for secure container access over the lifecycle of the application. Updates posted to the registry can be pulled automatically or manually by any legitimate host using the application — or set of applications — packaged in the container. (See Figure 2, previous page.)

The process of distributing the containers can be handled in several different ways. For example, an aircraft after landing can taxi to the maintenance area, connect to the service infrastructure at the airport, and pull any recently updated containers from the registry in the system server. The container updates will then be incorporated into the aircraft system. A vehicle equipped with modern wireless capabilities can be driving past a 5G base station, receive a transmission with updates in a container, and then proceed to install the updates automatically once the car is parked at home in the garage.

Because the technologies used in the VxWorks container implementation follow the OCI guidelines to the letter, developers know that containers they build will function reliably across infrastructures that are constructed according to the OCI standard. Proprietary solutions for software deployment, on the other hand, lack the agility and predictability of standards-based solutions and are generally unpopular in the industry for those reasons. In contrast, OCI-compliant tools — following both the Image Format specification and Runtime specification — effectively span the ecosystem composed of container platforms and container engines, as well as standards-based cloud provider environments and on-premises infrastructures.

> "We wanted to make sure that some of the key characteristics of VxWorks that are important — and the embedded systems on which VxWorks runs — are not altered. This is not about reducing performance; it is about keeping the same performance level and keeping the same DNA, ensuring the same determinism, and keeping a minimal footprint. The container engine is just under 400Kb total, with just under 100Kb for the actual container runtime."[4]
>
> — **Michel Chabroux, Senior Director,** *Product Management, Wind River*

4 *Expert Discussion: Cybersecurity and Container Usage for Avionics at the Intelligent Edge, Avionics International, March 3, 2021*

Ensuring Container Security

Security is a vital issue in any type of software deployment, and if container technology is to become successful in environments that call for heightened security — such as aerospace and defense, automotive applications, energy grids and subsystems, robotics implementations, and so on — extra measures for hardening solutions are needed.

Cloud-native, open-source registries typically provide a layer of security when using containers. For example, Harbor employs policies and role-based access control to secure container components. Each container image is scanned to ensure that it is free of known vulnerabilities and then signed as trusted before distribution. For sensitive, mission-critical deployments, Harbor provides a level of assurance when moving containers across cloud-native compute platforms.

Following DevSecOps software development best practices is one of the most effective means of protecting container security. The Department of Defense has published the Container Hardening Guide (October 2020), which outlines DevSecOps processes that are important for guarding against security breaches.

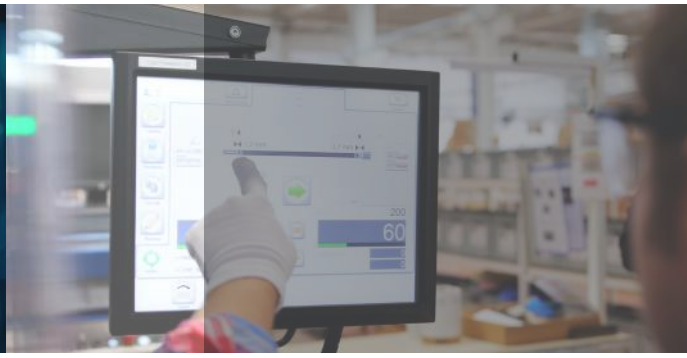
The VxWorks container engine takes advantage of security features available in VxWorks, including verifying digital signatures. System architects can develop a level of security consistent with the attack surface and operating environment in which a container is deployed. A range of protections is available, from initial boot operations through the power-down sequence. The principles of the CIA triad — confidentiality, integrity, and availability — represent the foundational concept upon which VxWorks container security is based.

45%

Global security tech leaders who say their company has sufficient security policies and tools in place for use of containers[5]

5 *Best Practices for Container Security, Forrester, July 2020*

A Confluence of Technologies Gives Birth to the Intelligent Edge



Computer solutions that are optimally suited for the intelligent edge are a growing need as more and more applications require low-latency, high-bandwidth performance to meet requirements.

To deliver the necessary degree of performance, the intelligent edge relies on several emerging technologies, including 5G networking, artificial intelligence and machine learning, IoT and mobility advances, and — increasingly — container technology.

Among the use cases in which containers can help resolve challenges at the edge are:

- **Manufacturing operations and industrial robotics:** AI-based automation is bolstered by compact, low-power installations that require the mission-critical reliability delivered by an embedded RTOS.
- **Innovative healthcare delivery:** Remote patient care, health monitoring systems, counseling, and other healthcare practices that have helped medical organizations deal with the COVID-19 pandemic can benefit from the security and agility of container technology.
- **Autonomous vehicles and smart city operations:** Lightweight, low-power operations are a vital factor in many embedded use cases involving AI-controlled vehicles, communication between vehicles, traffic flow monitoring, advanced driver assist systems (ADAS), and citywide warning and alert systems.
- **Retail customer personalization and communication:** Automated information kiosks, personalized signage displays, rich media product demonstrations, and online ordering systems can tap into the flexibility and power of container technology implemented at the intelligent edge.

> "The intelligent edge can benefit any business that manages infrastructure, networks, clouds, data centers, and connected endpoints such as sensors, actuators, and devices. It can support consumer use cases that require very low latency, such as cloud gaming and augmented and virtual reality. It can enable enterprise uses that require aggregating, securing, and analyzing a great deal of data across operations and customers. And it can improve industrial processes for managing quality, materials, and energy use, such as monitoring factory floors, assembly lines, and logistics."[6]
>
> — Deloitte Insights

6 *Arkenberg, Chris, Sanket S. Nesargi, Ariane Bucaille, Dan Littmann, "Gaining an Intelligent Edge: Edge Computing and Intelligence Could Propel Tech and Telecom Growth," Deloitte Insights, December 2020*

Using VxWorks-Based Containers in a Disaggregated Avionics System

The example depicted in Figure 3 shows how VxWorks containers enable a disaggregated system approach within a jet fighter in which multiple systems are linked from the edge to a centralized server, usually mounted close to the aircraft's center of gravity. The example highlights the streamlined software management that can be achieved in an environment within which multiple operating systems are present (including Wind River Linux and VxWorks), ensuring that applications can be reliably and securely managed over their full lifecycle.

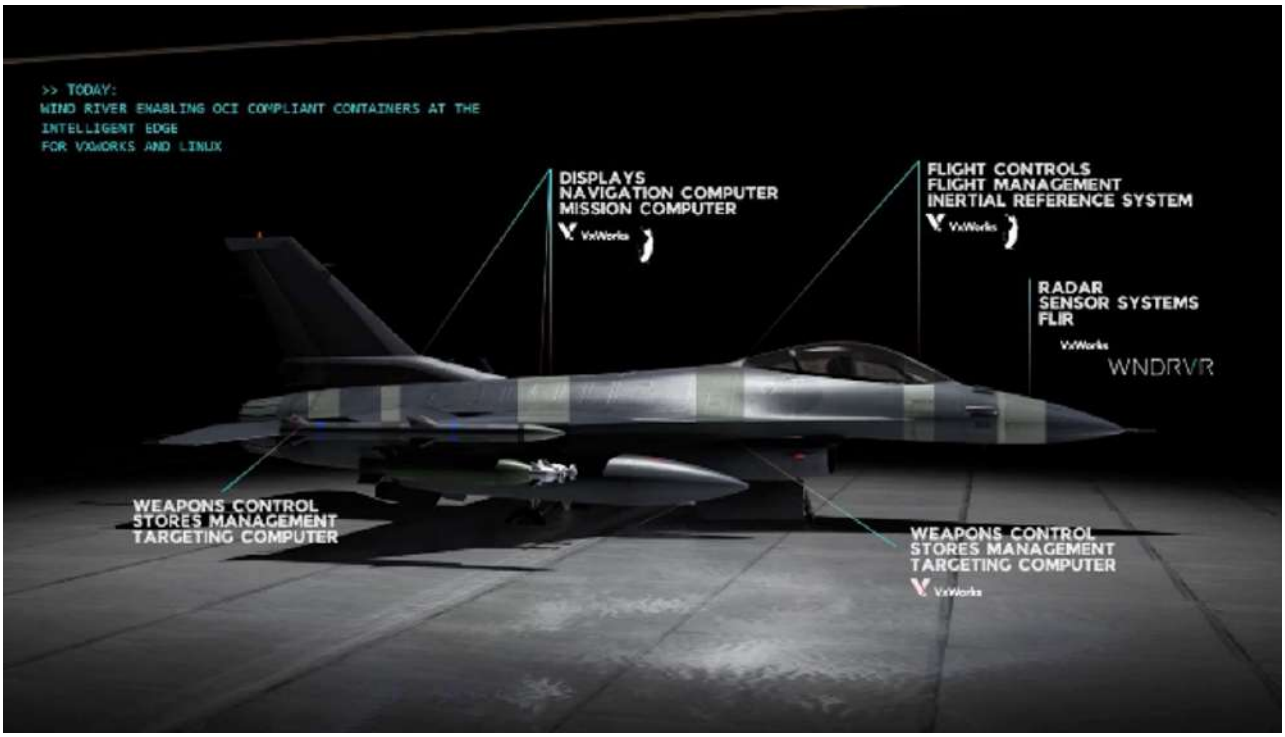
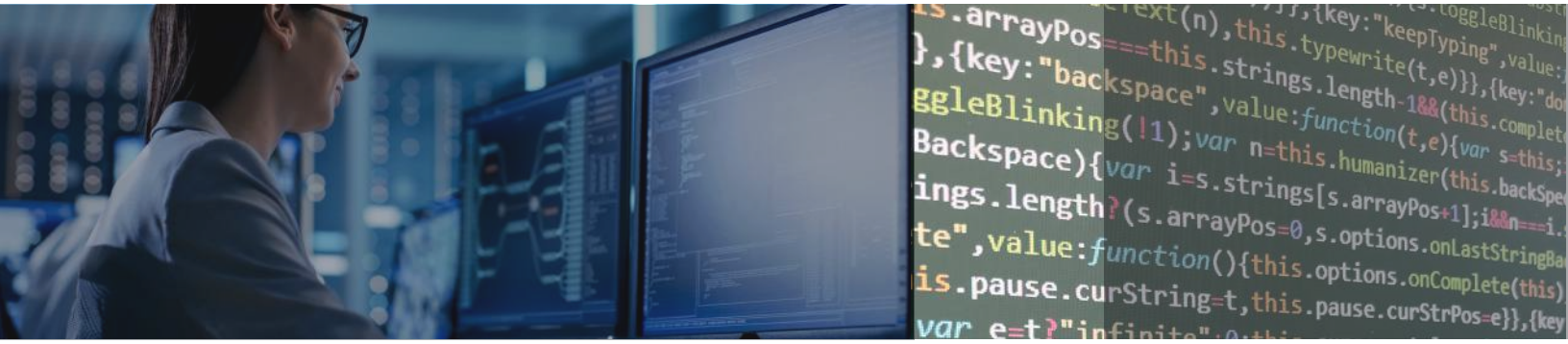


Figure 3. Disaggregated avionics system featuring VxWorks-based containers at the edge



To illustrate the process involved in performing a live container update on a running system, Wind River Senior Director of Product Management Michel Chabroux produced a video demonstration that depicts the process.

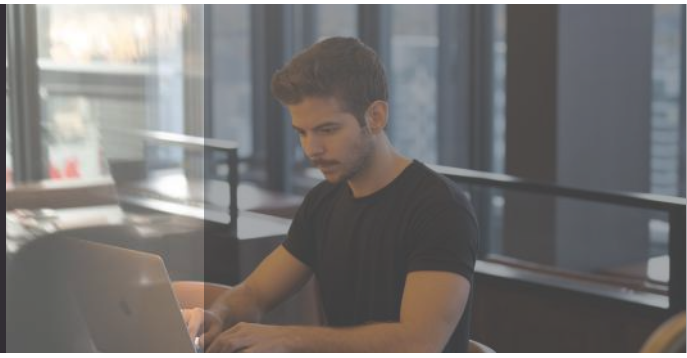
The demonstration shows a Python web server and simulates the need for an end-of-field update to be accomplished manually. "That update," Chabroux said, "consists of shutting down the application and retrieving the new version from the container registry." Docker Hub is used for the demonstration, but any other container registry deployed at the edge, such as Iron Bank, could be used as well. In the example, the container is pulled from the registry and restarted with a new version of the application.

Knowing the container is available, Chabroux continued, "we can now pull it directly from the running system. VxWorks at the edge is going to pull an OCI container just like you would do on any system." The data from Docker Hub confirms that the container has been downloaded. Logic can be employed verifying that the container has all the correct data.

The demonstration shows the ease with which a live VxWorks system can manage container deployment, updating an application that was shut down and then restarting the new version, operating in the same way container deployment is handled in a typical IT environment.

> " That update consists of shutting down the application and retrieving the new version from the container registry. We can now pull it directly from the running system. VxWorks at the edge is going to pull an OCI container just like you would do on any system. "
>
> — **Michel Chabroux, Senior Director, Product Management, Wind River**

Future Applications of VxWorks and Containers on the Edge



Opportunities for embedded applications and use cases at the intelligent edge have been expanded substantially by VxWorks container support.

The development makes it possible to deliver lightweight, low-power, low-latency solutions that satisfy demanding requirements across a wide swath of industry sectors. Going forward, 5G networks will become more prevalent, providing a ready means of distributing data (and containers) from the edge and linking local and central data centers using 3GHz cell towers and 28GHz small cells through fiber interconnects. This will further extend the potential of VxWorks-enabled solutions. These concepts can have a significant impact within the aerospace industry: Satellites, unmanned aircraft, communications, and mission flight control systems can be enhanced by secure, reliable access to the intelligent edge.

- **VxWorks:** The world's leading commercial real-time operating system (RTOS), VxWorks excels at high-performance aerospace and defense applications, industrial applications (including robotics and control automation), and intelligent vehicle applications. With the latest version providing support for containerization, VxWorks delivers compact RTOS capabilities for space and power-constrained embedded deployments. VxWorks meets the certification requirements for IEC 61508 SIL 3, ISO 26262 ASIL D, and IEC 62304.
- **VxWorks 653:** Built to meet the safety certifications of integrated modular avionics (IMA) operations, this version of VxWorks conforms with ARINC 653, supporting single-platform deployments of vital aeronautical applications. VxWorks 653 is certified conformant for the FACE™ Operating System Segment (OSS) Safety Base Profile.
- **Wind River Studio:** For intelligent edge deployments, Studio provides a full-featured, unifying infrastructure to complement and manage complex 5G edge networking installations. Studio developer capabilities are integrated to deliver the only full lifecycle management platform for intelligent systems at digital scale. Studio reengineers development workflows into solution sets that reduce development costs and accelerate capabilities for building, testing, and deploying on the edge.
- **Wind River Simics®:** This comprehensive system simulation environment streamlines design, development, and testing of complex edge computing systems and embedded solutions. Simics accommodates agile and DevSecOps software practices and enables teams to shorten development cycles and thoroughly test embedded system designs without physical hardware present.
- **Wind River Partner Ecosystem:** Third-party hardware and software solutions are available through an extensive partner ecosystem, offering a deep portfolio of capabilities to speed project development and reduce time-to-market.

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the intelligent transformation of mission-critical edge systems that demand the highest levels of security, safety, and reliability.